What is claimed is:

1. A method of visualizing information about the security of a network, the method comprising:

providing a 3-D visualization tool for simulating 3-D space on a two dimensional display device, said tool for accessing a database which relationally associates security events with network elements, wherein each said security event is associated with at least one of a plurality of categories of security events;

visually depicting at least some of said categories of security events in a first section of said simulated 3-D space;

visually depicting at least some of said network elements in a second section of said simulated 3-D space; and

displaying association lines in said 3-D simulated space between one or more displayed categories of security events and one or more displayed network elements.

2. The method according to claim 1, wherein said network elements are host computer systems.

3. The method according to claim 1, wherein said categories are represented by first graphical objects and said network elements are represented by second graphical objects, said association lines being drawn between various of said first and second graphical objects.

4. The method according to claim 3, wherein said second graphical object representing said network elements is an image of a geometric object.

5. The method according to claim 4, wherein different types of network elements are represented by varying one or more visual attributes or screen positions of the representative geometric objects.

6. The method according to claim 4, wherein said geometric object is associated with text describing the object.

7. The method according to claim 3, wherein said first graphical object is a position on a graph.

8. The method according to claim 3, wherein said first or second graphical object includes text.

9. The method according to claim 3, including visually depicting a trusted relationship line between the graphical object representing a first network element and the graphical object representing a second network element if the first network element can access data associated with the second network element.

10. The method according to claim 3, wherein said categories of security events are selected from the following group of event types: packet insertion, packet interception, application access, system file access, network access, denial of service, access permission, sniffing, security setup, impersonation, encryption, firewall.

11. The method according to claim 1, wherein said database includes:
temporal information reflecting a time at which each said security event occurred;
information relating to a first property of each network element; and
information relating to a second property of each network element.

12. The method according to claim 11, wherein said network elements are represented by geometric objects.

13. The method according to claim 11, wherein:

said first section of simulated 3-D space displays a first graph having a security event category axis and a temporal axis, each said displayed security event being visually indicated at a position on said graph corresponding to the category and time of the security event;

said second section of simulated 3-D space displays a second graph having an axis pertaining to said first property and an axis pertaining to said second property, said graphical objects representing said network elements being displayed on the graph at axes positions corresponding to the first and second properties thereof;

said association lines being drawn between said first graph and said second graph.

14. The method according to claim 13, wherein said association lines are drawn between positions of said first graph and said graphical objects representing said network elements.

15. The method according to claim 14, wherein:

the first property is organizational role information for correlating each network element with a role in, or department of, the organization; and

the second property is location information for indicating the physical location of each network element.

16. The method according to claim 13, including drawing a trusted relationship line between a graphical object representing a first network element and a graphical object representing a second network element if the first network element can access data associated with the second network element.

17. The method according to claim 13, including differentiating amongst various types of network elements by varying the visual attributes or screen positions of said graphical objects representing said network elements.

18. The method according to claim 13, including displaying the frequency of security events at various positions in said first graph.

19. The method according to claim 13, including:

storing in said database information about identities of attackers causing said security events;

visually depicting said attackers as geometrical objects in a third section of said simulated 3-D space; and

drawing association lines between said attackers and said security events.

20. The method according to claim 13, wherein said categories of security events are selected from the following group of event types: packet insertion, packet interception, application access, system file access, network access, denial of service, access permission, sniffing, security setup, impersonation, encryption, firewall.

21. A method of visualizing information about the security of a network, the method comprising:

recording security events and the network elements affected thereby;

associating each security event with at least one of a plurality of categories of security events;

providing a 3-D visualization tool for simulating 3-D space on a two dimensional display device, and using said tool:

visually depicting at least some of the categories of security events in a first section of simulated 3-D space;

visually depicting at least some of the network elements in a second section of simulated 3-D space; and

drawing association lines between one or more displayed categories of security events and one or more displayed network elements affected thereby.

22. The method according to claim 21, comprising:

recording a time at which each security event occurred;

associating each network element with at least two properties;

displaying in the first section of simulated 3-D space a first grid of cells, each cell being associated with a security event category and a temporal value, the security events being visually indicated by the cells of the first grid; and

displaying in the second section of simulated 3-D space a second grid of cells, each cell being associated with an instance of the first property and an instance of the second property, wherein each displayed network element is represented by a geometric object disposed at a cell of the second grid that corresponds to the first and second properties of the network system;

said association lines being drawn between cells of the first grid and cells of the second grid.

23. The method according to claim 22, wherein the first property is an organizational role of the network element, and the second property is a physical location of the network element.

24. The method according to claim 22, including drawing a trusted relationship line between a graphical object representing a first network element and a graphical object representing a second network element if the first element can access data associated with the second element.

25. The method according to claim 22, including differentiating amongst various types of network elements by varying the visual attributes or screen positions of the respective geometric objects.

26. The method according to claim 22, including displaying the frequency of security event at the cells of the first grid.

27. The method according to claim 22, including:

recording identities of attackers causing the security events;

visually depicting the attackers as geometrical objects in a third section of the simulated 3-D space; and

drawing association lines between the attackers and the security events.

28. A method of visualizing information about the security of a network, the method comprising:

recording security events and the network elements affected thereby;

recording a time at which each security event occurred;

associating each security event with at least one of a plurality of categories of security events;

associating each network element with one or more additional properties;

providing a 3-D visualization tool for simulating 3-D space on a two dimensional display device, and using said tool:

displaying a first grid of cells in the simulated 3-D space, each cell being associated with a security event category and a temporal value, the security events being visually indicated by the cells of the first grid;

displaying a second grid of cells in the simulated 3-D space, each cell being associated with at least one of said properties, wherein each displayed network element is represented by a geometric object disposed at a cell of the second grid that corresponds to the value of said at least one property; and

drawing association lines between one or more displayed security events and one or more displayed network elements affected thereby.

29. The method according to claim 28, including:

recording identities of attackers causing the security events;

visually depicting the attackers as geometrical objects in the simulated 3-D space; and

drawing association lines between the attackers and the security events.

30. Software for visualizing information about the security of a network, wherein security events and the network elements affected thereby are recorded in a database, each said security event being associated with at least one of a plurality of categories of security events, the software comprising code for:

interfacing with the database;

simulating 3-D space on a two dimensional display device;

visually depicting at least some of said categories of security events in a first section of said simulated 3-D space;

visually depicting at least some of said network elements in a second section of said simulated 3-D space; and

drawing association lines in said 3-D simulated space between one or more displayed categories of security events and one or more displayed network elements affected thereby.

31. Software for visualizing information stored in a database about the security of a network, wherein said database records:

security events and the network elements associated therewith, each security event being associated with at least one of a plurality of categories of security events, each network element being associated with at least one property; and

a time at which each security event occurred;

the software having code for:

simulating 3-D space on a two dimensional display device;

displaying a first grid of cells in the simulated 3-D space, each cell being associated with a security event category and a temporal value, the security events being visually indicated by the cells of the first grid;

displaying a second grid of cells in the simulated 3-D space, each cell being associated with an instance of a said at least one property, wherein a geometric object representing a displayed network element is disposed at a corresponding cell of the second grid; and

drawing association lines between one or more displayed security events and one or more displayed network elements associated therewith.